National Infrastructure
Advisory Council (NIAC)

Intelligence Coordination Working Group

Status Report
July 12, 2005

John Chambers **President & CEO,** **Cisco Systems, Inc.**	**Gilbert Gallegos** **Retired Chief of Police** **Albuquerque, NM**

To Review……

- ☐ Purpose
- ☐ Working Group Focus
- ☐ Pending Actions

Purpose

Develop policy recommendations that ensure:

- ☐ Intelligence Community (IC) (including Law Enforcement) understands private sector's Critical Infrastructure Protection (CIP) domain expertise, intelligence requirements, and dissemination capabilities

- ☐ Private sector understands IC responsibilities, objectives and processes in CIP, especially regarding threat assessments

- ☐ Improvements in IC and private sector interaction for CIP are understood and considered by policymakers

---

NIAC IC Working Group Focus

- ☐ In what ways can the Intelligence Community (IC) help the private sector?

- ☐ In what ways can the private sector help the IC?

Working Group Approach

☐ Objective: Make recommendations to the President which will enhance government and private-sector contributions to CIP

☐ Analyze current information flows among appropriate IC and private sector elements and identify gaps

☐ Determine how to obtain and share information required (but not yet available) for CIP

☐ Focus efforts around the seven stages of the <u>Infrastructure Risk Management Spectrum of Actions</u> of the NIPP:
  ■ Deterrence, Prevention, Protection, Preparedness, Crisis Management and Response, Recovery, and Restoration

5

Update from April Quarterly

Completed/Ongoing Actions:

☐ Collecting private-sector requirements and analyzing them for IC information-sharing needs and issues

☐ Collecting and analyzing IC requirements for CIP information and expertise sharing

☐ Examining Law Enforcement/CIP information and incident reporting mechanisms (DHS/IA lead)

☐ Hosted unprecedented IC – private-sector CIP working session with over 30 senior executives, key representatives, and working-level staff to delve into issues and continue deeper dialog. Second working session planned for late July timeframe.

6

Next Steps

Refining Intelligence Information Sharing Needs

- ☐ What to share? (how will information be used – context)
- ☐ Who should share?
- ☐ How to share? (information as well as expertise)
- ☐ "Protected Critical Infrastructure Information (PCII)" program issues and gaps
- ☐ Additional requirements (clearances, architectures, networks)
- ☐ Shift CIP mindset to a "Need to Share" model

Next Steps (continued)

- ☐ Complete analysis of requirements collected from sectors and agencies
- ☐ Map information-sharing gaps to the seven steps in the National Infrastructure Protection Plan (NIPP)
- ☐ Develop draft recommendations for the President

Discussion

- ☐ Questions?